

1 We claim:

2 1. In a processing system including a server capable of communicating with a client

3 via a communications channel, a method of authenticating a data object, the

4 method comprising the steps of, in the server,

5 (1) receiving the data object transmitted from the client to the server via  
6 the communications channel;

7 (2) generating a signature by processing the data object;

8 (3) associating the signature with the data object to create a signed object;

9 and

10 (4) authenticating the signed object, subsequently upon request, by:

11 (a) deriving from the signed object information representative of  
12 the data object and the signature,

13 (b) generating a comparison value using the information  
14 representative of the data object,

15 (c) determining whether the comparison value and at least a  
16 portion of the signature meet a pre-determined criteria.

17

18 2. The method of claim 1 wherein the data object comprises a document.

19

20 3. The method of claim 1 including the further step of, in the server, authenticating  
21 the client.

22

1 4. The method of claim 3 wherein the client is authenticated by the server using  
2 information representative of the client.

3

4 5. The method of claim 4 wherein the information representative of the client  
5 comprises a password provided by the client.

6

7 6. The method of claim 3 wherein the client is authenticated by the server using an  
8 encrypted data channel.

9

10 7. The method of claim 6 wherein the encrypted data channel utilizes a SSL  
11 protocol.

12

13 8. The method of claim 3 wherein the client is authenticated by the server using a  
14 public key-based processing step.

15

16 9. The method of claim 8 wherein the public key-based processing step includes the  
17 presentment of a client certificate.

18

19 10. The method of claim 9 wherein the client and server mutually authenticate using a  
20 zero-knowledge proof step.

21

22 11. The method of claim 3 including the further step of, in the server, creating and  
23 managing private keys to use in the step of generating the signature.

1 12. The method of claim 11 wherein the server assigns a private key to the client.

2

3 13. The method of claim 12 wherein the private key assigned to the client is  
4 determined based upon the information representative of the client.

5

6 14. The method of claim 13 wherein the step of generating the signature includes the

7 steps of:

8 assigning a private key to the client;

9 performing a predefined hash function on the data object to produce a hash total;

10 and

11 encyphering the hash total using the private key.

12

13 15. The method of claim 1 wherein the signed object comprises the signature and an  
14 address of the data object.

15

16 16. The system of claim 1 wherein the signed object comprises the signature and the  
17 data object.

18

19

1       17. In a processing system comprising a server capable of communicating with a  
2           client via a communications channel, a method of generating a digital signature,  
3           the method comprising the steps of, in the server:

4               receiving a data object transmitted from the client to the server via the  
5           communications channel;

6               assigning to the data object a descriptor containing a property field, the  
7           property field containing a signature field;

8               assigning a private key, stored at the server, to the client;

9               processing the data object using a pre-determined hash function and the  
10           private key to generate a signature; and

11               attaching the signature to the signature field associated with the data  
12           object to create a signed object.

13  
14       18. The method of claim 17 including the step of, in the server, authenticating the  
15           signed object by verifying the signature attached to the signature field of the  
16           signed object.

17

1 19. The method of claim 18 wherein the verifying step further comprises the steps of:

2 (a) obtaining the data object from the signed object;

3 (b) obtaining the signature from the signed object;

4 (c) obtaining the private key stored at the server used to generate the

5 signature;

6 (d) processing the data object using a pre-determined hash function and

7 the private key to generate a comparison value; and

8 (e) determining whether the comparison value and at least a portion of

9 the signature meet a pre-determined criteria.

11 20 The method of claim 19 wherein the property field further comprises a timestamp.

13 21. The method of claim 20 wherein the property field further comprises an identifier  
14 used to look up a key stored at the server.

16 22. The method of claim 19 wherein the property field further comprises key  
17 information used to generate the comparison value.

19 23. The method of claim 17 wherein the descriptor further comprises a plurality of  
20 property fields.

22 24. The method of claim 23 wherein at least one of the property fields further  
23 comprises data that is private to the server.

1 25. The method of claim 23 wherein at least one of the property fields further  
2 comprises additional data that is signed by a key private to the server.  
3

4 26. The method of claim 25 wherein the additional data is derived by processing the  
5 data object using a pre-determined function.  
6

7 27. The method of claim 26 wherein the pre-determined function is a hash function.  
8

9 28. The method of claim 26 wherein the pre-determined function is a transform  
10 function.  
11

12 29. The method of claim 25 wherein the additional data is obtained from a device.  
13

14 30. The method of claim 29 wherein the device receives the data object prior to  
15 subsequent processing by the server.  
16

17 31. The method of claim 29 wherein the device does not receive the data object.  
18

19 32. The method of claim 29 wherein the device further comprises a device for  
20 generating a timestamp.  
21

22 33. The method of claim 29 wherein the additional data, after being obtained from the  
23 device, is used by the server to generate the signature.  
24

1       34. A method of transmitting transaction objects between a client and a server capable  
2           of communicating with the client via a communications channel, the method  
3           comprising the steps of:

4           receiving at the client, from the server, an HTML object having a header record  
5           and an HTML form tag distinct from the header record, the HTML form tag  
6           having an outformat field representative of an outgoing transmission  
7           cryptographic protocol,  
8           receiving, at the client, input form data corresponding to the HTML form tag,  
9           generating secure form data by applying the specified outgoing transmission  
10           security cryptographic protocol of the HTML form tag to the input form data, and  
11           transmitting to the server a return message including the secure form data.

12

13       35. A computer implemented method of providing a digital signature system on a  
14           server for use by a remote client, the method comprising:

15           generating on the server a private key for a user on the client;  
16           storing on the server the private key for the user;  
17           generating a digital signature using the stored private key for a data object  
18           provided by the user; and  
19           sending the digital signature to the client.

20

21       36. The method of claim 35 wherein the digital signature is contained within a signed  
22           object.

23

37. The method of claim 36 wherein generating the digital signature step further comprises:

performing a pre-defined hash function on the data object to create a hash and

performing a pre-defined encryption function using the private key on the value.

38. The method of claim 37 wherein the signed object comprises the digital signature and an address of the data object.

39. The method of claim 37 wherein the signed object comprises the digital signature and the data object.

40. The method of claim 37 wherein the signed object comprises the digital signature contained within the data object.

41. The method of claim 36 wherein the signed object comprises a hash of the data object contained within the digital signature.

42. The method of claim 37, further including, on the server:  
verifying the digital signature upon request by the client.

1       43. The method of claim 42 wherein verifying the digital signature further comprises:  
2           receiving the signed object from the client;  
3           obtaining the data object using information contained within the signed object;  
4           obtaining the digital signature using information contained within the signed  
5           object;  
6           obtaining the private key stored on the server using information contained within  
7           the signed object;  
8           generating a comparison value using the data object;  
9           verifying the digital signature if the comparison value and at least a portion of the  
10          digital signature meet a pre-determined criteria.

11  
12       44. The method of claim 43 wherein the signed object comprises the digital signature  
13          and an address of the data object.

14  
15       45. The method of claim 43 wherein the signed object comprises the digital signature  
16          and the data object.

17  
18       46. The method of claim 43 wherein the signed object comprises the digital signature  
19          contained within the data object.

20  
21       47. The method of claim 43 wherein the signed object comprises a hash of the data  
22          object contained within the digital signature.

23

1 48. The method of claim 35 further comprising, authenticating a user, by the server,  
2 before providing access to the system.

3

4 49. The method of claim 48 wherein authenticating a user further comprises receiving  
5 a user ID and a password from the client.

6

7 50. The method of claim 49 further comprising assigning, by the server, a private key  
8 to the client based upon the user ID.

9

10 51. The method of claim 35 further comprising assigning, by the server, a private key  
11 to the client based upon a system policy and data obtained from the client.

12

13 52. The method of claim 50 wherein the digital signature further comprises:  
14 a encrypted field; and  
15 a timestamp,  
16 wherein the server generates the encrypted field by hashing the data object according  
17 to a predefined hash function to create a hash, and encrypting the hash using the  
18 private key assigned to the user.

19

20 53. The method of claim 52 wherein the digital signature further comprises a server  
21 key.

22

1 54. The method of claim 43 further including generating a verification response at the  
2 server and transmitting the verification response to the client.

3

4 55. The method of claim 54 further including generating a verification signature for  
5 the verification response at the server and transmitting the verification signature  
6 to the client.

7

8 56. A digital signature system including:

9 a server capable of communicating with a client via a communications channel, and  
10 means for authenticating a data object, further comprising:

11 (1) means for receiving the data object transmitted from the client to the  
12 server via the communications channel;

13 (2) means for generating a signature by processing the data object;

14 (3) means for associating the signature with the data object to create a  
15 signed object; and

(4) means for authenticating the signed object, subsequently upon request,

17 by: (a) deriving from the signed object information representative of  
18 the data object and the signature.

19 (b) generating a comparison value using the information  
20 representative of the data object.

21 (c) determining whether the comparison value and at least a  
22 portion of the signature meet a pre-determined criteria.

1 57. The system of claim 56 wherein the data object comprises a document.

2

3 58. The system of claim 56 further comprising means for obtaining information  
4 representative of the client to authenticate the client.

5

6 59. The system of claim 58 further comprising means for creating and managing  
7 private keys used to generate the signature.

8

9 60. The system of claim 59 further comprising means for assigning a private key to  
10 the client.

11

12 61. The system of claim 60 wherein the private key is assigned to the client using the  
13 information representative of the client.

14

15 62. The system of claim 56 wherein the means for generating a signature further  
16 comprise:

17 assigning a private key to the client;

18 performing a predefined hash function on the data object to produce a hash total;

19 and

20 encyphering the hash total using the private key.

21

22 63. The system of claim 56 wherein the signed object comprises the signature and an  
23 address of the data object.

1       64. The system of claim 56 wherein the signed object comprises the signature and the  
2                   data object.

3

4       65. A processing system comprising:

5                   a server capable of communicating with a client via a communications channel,  
6                   processing means in the server for generating a digital signature, further  
7                   comprising:

8                   means for receiving a data object transmitted from the client to the server  
9                   via the communications channel;

10                  means for assigning to the data object a descriptor containing a property  
11                  field, the property field containing a signature field;

12                  means for assigning a private key, stored at the server, to the client;

13                  means for processing the data object using a pre-determined hash function  
14                  and the private key to generate a signature; and

15                  means for attaching the signature to the signature field associated with the  
16                  data object to create a signed object.

17

18       66. The processing system of claim 65 further comprising means for authenticating  
19                  the signed object.

20

21       67. The processing system of claim 66 wherein the means for authenticating the  
22                  signed object is further comprised of means for verifying the signature attached to  
23                  the signature field of the signed object.

24

1 68. The processing system of claim 67 wherein the means for verifying further  
2 comprises:

3 (a) means for obtaining the data object from the signed object;

4 (b) means for obtaining the signature from the signed object;

5 (c) means for obtaining the private key stored at the server used to

6 generate the signature;

7 (d) means for processing the data object using a pre-determined hash

8 function and the private key to generate a comparison value; and

9 (e) means for determining whether the comparison value and at least a

portion of the signature meet a pre-determined criteria.

11

12 69. The processing system of claim 67 wherein the property field further comprises a  
13 timestamp.

14

15 70. The processing system of claim 67 wherein the property field further comprises  
16 an identifier used to look up a key stored at the server.

17

18 71. The processing system of claim 67 wherein the property field further comprises  
19 key information used to generate the comparison value.

20

21 72. The processing system of claim 67 wherein the descriptor further comprises a  
22 plurality of property fields

1 73. The processing system of claim 72 wherein at least one of the property fields  
2 further comprises data that is private to the server.

3

4 74. The processing system of claim 72 wherein at least one of the property fields  
5 further comprises additional data that is signed by a key private to the server.

6

7 75. The processing system of claim 74 wherein the additional data is derived by  
8 processing the data object using a pre-determined function.

9

10 76. The processing system of claim 75 wherein the pre-determined function is a hash  
11 function.

12

13 77. The processing system of claim 75 wherein the pre-determined function is a  
14 transform function.

15

16 78. The processing system of claim 74 further comprising a device for providing the  
17 additional data.

18

19 79. The processing system of claim 74 wherein the device receives the data object  
20 prior to subsequent processing by the server.

21

22 80. The processing system of claim 74 wherein the device does not receive the data  
23 object.

1  
2 81. The processing system of claim 74 wherein the device further comprises a device  
3 for generating a timestamp.

4  
5 82. The processing system of claim 74 wherein the server generates the signature  
6 after obtaining the the timestamp from the device.

7  
8 83. A digital signature system for use by a remote client, the system comprising:  
9 a server computer;

10 processing means on the server for generating a private key for a user on the  
11 client;

12 storing means on the server for storing the private key for the user;

13 processing means for generating a digital signature using the stored private key  
14 for a data object provided by the user; and

15 transmitting means for sending the digital signature from the server to the client.

16  
17 84. The digital signature system of claim 83 wherein the digital signature is contained  
18 within a signed object.

19  
20 85. The digital signature system of claim 84 wherein the processing means for  
21 generating the digital signature further comprise:

22 means for performing a pre-defined hash function on the data object to  
23 create a hash value; and

1 means for performing a pre-defined encryption function using the private  
2 key on the hash value.

3

4 86. The digital signature system of claim 85 wherein the signed object comprises the  
5 digital signature and an address of the data object.

6

7 87. The digital signature system of claim 85 wherein the signed object comprises the  
8 digital signature and the data object.

9

10 88. The digital signature system of claim 85 wherein the signed object comprises the  
11 digital signature contained within the data object.

12

13 89. The digital signature system of claim 85 wherein the signed object comprises a  
14 hash of the data object contained within the digital signature.

15

16 90. The digital signature system of claim 85, further comprising:  
17 verifying the digital signature upon request by the client.

18

19

1 91. The digital signature system of claim 90 wherein the means for verifying the  
2 digital signature further comprises:  
3 means for receiving the signed object from the client;  
4 means for obtaining the data object using information contained within the signed  
5 object;  
6 means for obtaining the digital signature using information contained within the  
7 signed object;  
8 means for obtaining the private key stored on the server using information  
9 contained within the signed object;  
10 means for generating a comparison value using the data object;  
11 means for verifying the digital signature if the comparison value and at least a  
12 portion of the digital signature meet a pre-determined criteria.  
13  
14 92. The digital signature system of claim 91 wherein the signed object comprises the  
15 digital signature and an address of the data object.  
16  
17 93. The digital signature system of claim 91 wherein the signed object comprises the  
18 digital signature and the data object.  
19  
20 94. The digital signature system of claim 91 wherein the signed object comprises the  
21 digital signature contained within the data object.  
22

1 95. The digital signature system of claim 91 wherein the signed object comprises a  
2 hash of the data object contained within the digital signature.

3

4 96. The digital signature system of claim 91 further comprising means for  
5 authenticating a user before providing access to the system.

6

7 97. The digital signature system of claim 96 wherein means for authenticating a user  
8 further comprises means for receiving a user ID and a password from the client.

9

10 98. The digital signature system of claim 97 wherein the server assigns a private key  
11 to the client based upon the user ID.

12

13 99. The digital signature system of claim 98 wherein the server assigns a private key  
14 to the client based upon a system policy and data obtained from the client.

15

16 100. The digital signature system of claim 91 wherein the digital signature further  
17 comprises:  
18 a encrypted field; and  
19 a timestamp,  
20 wherein the server generates the encrypted field by hashing the data object according  
21 to a predefined hash function to create a hash, and encrypts the hash using the private  
22 key assigned to the user.

1 101. The digital signature system of claim 91 wherein the digital signature further  
2 comprises a server key.

3

4 102. The digital signature system of claim 100 further comprising:  
5 means for generating a verification response at the server; and  
6 means for transmitting the verification response to the client.

7

8 103. The digital signature system of claim 100 further comprising:  
9 means for generating a verification signature for the verification response at the  
10 server; and  
11 means for transmitting the verification signature to the client.

12